MITCHELL | HAMLINE School of Law

Cybaris®

Volume 8 | Issue 2 Article 3

2017

Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property to Keep Our Ports, Facilities, and Vessels Safe from Cyber Threats

Rachel Foote

CYBERSECURITY IN THE MARINE TRANSPORTATION SECTOR: PROTECTING INTELLECTUAL PROPERTY TO KEEP OUR PORTS, FACILITIES, AND VESSELS SAFE FROM CYBER THREATS

BY RACHEL FOOTE[1]

I. INTRODUCTION AND BACKGROUND 232
A. The Importance of Marine Transportation 234
B. The Necessity of Integrated Systems in the Maritime Industry 237
C. The Gravity of the Cyber Threat 238
II. CURRENT GOVERNMENT REGULATIONS AND APPROACHES 239
A. Marine Transportation 239
1. Maritime Transportation Security Act of 2002 240
2. Port Security Grant Program 242
B. Critical Infrastructure 243
1. Executive Order 13636 and Presidential Policy Directive 21 244
2. National Institute of Standards and Technology Cybersecurity Framework 245
3. United States Coast Guard Cyber Strategy 247
C. Recent Cybersecurity Legislation 248
1. 2014 Cybersecurity Legislation 248
a. National Cybersecurity Protection Act of 2014 249
b. Cybersecurity Enhancement Act of 2014 250
2. Cybersecurity Act of 2015 and Recent Presidential Policy 251
a. Cybersecurity Act of 2015 251
b. 2016 Presidential Policy 252
III. MARITIME INDUSTRY PRACTICE AND GUIDANCE 255
A. Baltic and International Maritime Council: The Guidelines on Cyber Security Onboard Ships 255
B. International Maritime Organization: Interim Guidelines on Maritime Cyber Risk Management 258
C. American Bureau of Shipping Guidance Notes 259
IV. RECOMMENDATIONS 262
A. Create a Culture of Cyber Risk Awareness 262
B. Ensure MTSA Required Plans Address Cyber Risk 262
C. Develop Additional Maritime Focused Cybersecurity Legislation 263
V. CONCLUSION 264

[1] Rachel Foote is a part-time Juris Doctor candidate at Mitchell Hamline School of Law, expected to graduate in 2019. She is also an active duty member of the U.S. Coast Guard. The views presented in this article are those of the author alone and do not represent the views of the Coast Guard. The author would like to thank Professor Sharon Sandeen and the entire Cybaris editorial board for their feedback and support.

I. INTRODUCTION AND BACKGROUND

In the time of wooden sailing ships and docks, the tide, currents, and available manpower were the forces that had the most profound effect on marine transportation.[2] Today, ships, ports, and facilities are run by sophisticated computers and software systems. These systems control, among other things, vessel engines,[3] navigation,[4] and facility automation.[5] While many of these systems are covered by patents[6] and involve trade secrets,[7] they remain vulnerable to cyber-attacks because of their increasingly integrated nature. Indeed, depending on the target and level of severity, a cyber-attack could cause serious economic[8] and environmental impacts. For example, the Exxon Valdez grounding, which caused one of the largest oil spills in U.S. history, involved a release of 257,000 barrels of oil from a total of 1.2 million barrels that the vessel was carrying.[9] For comparison, modern crude oil carriers can carry up to 2.2 million barrels of crude oil.[10] A cyber-attack that successfully disrupted a crude carrier's navigation or steering, resulting in the vessel grounding, could cause an oil spill much more devastating than Exxon Valdez.

---

[2] Chris Oxlade, *History of Sailing Ships*, Q-FILES, https://www.q-files.com/technology/ships-and-boats/history-of-sailing-ships/ (last visited Nov. 8, 2016).

[3] *Automation and Marine Software*, ABB, http://new.abb.com/marine/systems-and-solutions/automation-and-marinesoftware (last visited Nov. 11, 2016) (ABB is an industrial technology company that sells marine software for monitoring and automation on vessels).

[4] TALK OF THE NATION: SCIENCE FRIDAY, HOW LARGE SHIPS USE NAVIGATION SYSTEMS (Nat'l Pub. Radio Jan. 20, 2012). http://www.npr.org/2012/01/20/145525012/how-large-ships-use-navigation-systems.

[5] U.S. GOV'T ACCOUNTABILITY OFFICE GAO-14-459, MARITIME CRITICAL INFRASTRUCTURE PROTECTION: DHS NEEDS TO BETTER ADDRESS PORT CYBERSECURITY 4 (2014) ("maritime stakeholders rely on numerous types of information and communications technologies to manage the movement of cargo throughout ports.").

[6] *Cf.* Press Release, ABB, ABB Again Heads List for Most Patent Applications Filed by a Swiss-based Company (Feb. 26, 2015), http://www.abb.com/cawp/seitp202/67a510c11e3e4656c1257df7005309a2.aspx (last visited Feb. 3, 2017).

[7] *See, e.g.*, L-3 Comm. Westwood Corp. v. Robichaux, No. 06-279, 2008 WL 577560 (E.D. La. Feb. 29, 2008).

[8] Matthew Chambers & Mindy Liu, *Maritime Trade and Transportation by the Numbers*, U.S. DEP'T OF TRANSP., http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/by_the_numbers/maritime_trade_and_transportation/index.html (last visited Oct. 22, 2016) (according to 2011 data, 53% of U.S. import value and 38% of U.S. export value was by vessel, the largest share of any mode of transportation); Lily Hay Newman, *What if a Cybersecurity Attack Shut Down Our Ports?*, SLATE (May 11 2015, 11:16 AM), http://www.slate.com/articles/technology/future_tense/2015/05/maritime_cybersecurity_ports_are_unsecured.html (last visited Nov. 11 2016) ("90 percent of the world's goods are shipped on boats.").

[9] *Oil Spill Facts: Questions and Answers About the Spill*, EXXON VALDEZ OIL SPILL TRUSTEE COUNCIL, http://www.evostc.state.ak.us/%3FFA=facts.QA (last visited Nov. 1, 2016).

[10] *Today in Energy: September 16, 2014*, U.S. ENERGY INFO. ADMIN., http://www.eia.gov/todayinenergy/detail.php?id=17991 (last visited Oct. 22, 2016) (very large crude carriers are responsible for most global crude oil shipments, and carry between 1.9 million and 2.2 million barrels of crude oil).

This significant and developing threat to the marine transportation sector has been the subject of comparatively little regulation and guidance. While parts of the Maritime Transportation and Security Act of 2002 (MTSA) can be read to include cyber vulnerabilities, the Act was not originally written with this threat in mind.[11] In February 2016, the Baltic and International Maritime Council (BIMCO) and several other influential maritime associations released "The Guidelines on Cyber Security Onboard Ships."[12] The International Maritime Organization (IMO) followed suit in June 2016, releasing interim guidelines addressing cyber risk.[13] Additionally, the American Bureau of Shipping (ABS) released a series of volumes addressing cybersecurity for marine and offshore facilities, the first published in February 2016.[14]

Given that maritime cybersecurity is a relatively new area of emphasis, this Note will look to develop a foundation from which to build future research and recommendations. This Note will first provide an overview of the maritime industry and highlight industry reliance on integrated systems. Section II will survey current United States government regulations and approaches, including methods found in the critical infrastructure sector. Section III will examine the recently promulgated industry guidance. From this data, this Note will posit some basic procedural, regulatory, and legislative suggestions to assist the maritime industry in continuing to protect its critical intellectual property and to ensure the safety of vessels and United States ports.

[11] Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064 (2002) ("An Act To amend the Merchant Marine Act, 1936, to establish a program to ensure greater security for United States seaports, and for other purposes.").
[12] BALTIC & INT'L MAR. COUNCIL, *infra* note 224.
[13] INT'L MAR. ORG., *infra* note 251.

A. The Importance of Marine Transportation

According to findings for the 2002 Maritime Transportation and Security Act, the United States has 361 public ports.[15] Maritime ports in the U.S. handle over $1.3 trillion in cargo annually.[16] A significant disruption of the marine transportation sector would cause severe economic complications, especially if it impacted one of our top twenty-five ports.[17] Ports and port facilities are vulnerable to cyber-attacks because they rely on communications and information technologies to achieve cargo movement within the port.[18] These systems include terminal operating systems, industrial control systems, business operations systems, and access control and monitoring systems.[19] In 2014, "a major U.S. port facility suffered a system disruption which shut down multiple ship-to-shore cranes for several hours."[20] Protection of Maritime Critical Infrastructure[21] is crucial for American prosperity and security. A cyber-attack at a port could have a ripple effect that impacts other critical infrastructure sectors.[22]

Marine transportation is not specifically called out as one of the sixteen critical infrastructure sectors[23] identified in Presidential Policy Directive Twenty-One, however, it can be considered a subset of the "Transportations Systems" sector.[24] All of the sectors rely, to a certain degree, on the goods that make their way through U.S. ports.[25] However, the sectors most likely to be significantly affected by a port disruption are Transportation Systems, Critical Manufacturing, Chemical, Energy, Food and Agriculture, and Commercial Facilities.[26]

---

[14] 1 AMERICAN BUREAU OF SHIPPING, *infra* note 264.
[15] Maritime Transportation Security Act § 101(1) (2002).
[16] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4 at 1.
[17] Maritime Transportation Security Act § 101(5) ("Twenty-five United States ports account for 98 percent of all container shipments.").
[18] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 4 at 4.
[19] *Id.* at 4–5.
[20] U.S. COAST GUARD, CYBER STRATEGY 17 (2015), https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf.
[21] *Id.* at 31 ("Maritime Critical Infrastructure includes the ports, facilities, vessels, and related systems that facilitate trade within the U.S., support national defense and homeland security objectives, and connect the Nation to the global supply chain.").
[22] OFFICE OF CYBER & INFRASTRUCTURE ANALYSIS, CONSEQUENCES TO SEAPORT OPERATIONS FROM MALICIOUS CYBER ACTIVITY 12-16 (March 3, 2016, 13:00 EST), https://public.intelligence.net/dns-seaport-cyber-attacks.
[23] The White House, Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (the sectors are: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, and Water and Wastewater Systems).
[24] *Id.*
[25] OFFICE OF CYBER & INFRASTRUCTURE ANALYSIS, *supra* note 21.
[26] *Id.*

A large number of industries included in the critical manufacturing sector are dependent "upon 'just-in-time' supply chains."[27] These industries can be significantly impacted by a disruption in port operations, leading to an interruption of the supply chain.[28] This could force companies within this sector to reduce or even halt production until port operations are normalized or another source of supply (not involving the impacted port(s)) is found.[29]

Another sector that relies on "just-in-time" supplies is the commercial facilities sector.[30] Companies in this sector keep limited inventory on hand, thus a port disruption could negatively impact business by disrupting the supply chain.[31] Indeed, it was projected that the West Coast ports labor slowdown in 2014–2015 "would cost the retail industry $7 billion in 2015 . . . due to missed sales, below optimal inventory levels, and the higher price of moving goods during the slowdown."[32]

The food and agriculture sector would also be negatively impacted by a maritime industry disruption.[33] In 2014, sixty-five percent of agricultural imports and seventy-three percent of exports were waterborne.[34] Temporary restrictions or closures of ports or waterways can increase product spoilage, leading to lost sales, and cause diversion to other transportation modes or ports, leading to higher transportation costs.[35] Additionally, a port disruption could lead to a shortage of products that are traditionally imported, such as sugar, coffee, and certain fruits and vegetables.[36]

[27] *Id.* at 12.
[28] *Id.*
[29] *Id.*
[30] OFFICE OF CYBER & INFRASTRUCTURE ANALYSIS, *supra* note 21 at 12.
[31] *Id.*
[32] *Id.* (*citing* Courtney Reagan, *West Coast Ports: Retail's $7 Billion Problem*, CNBC (Feb. 9, 2015, 12:58 PM), http://www.cnbc.com/2015/02/09/west-coast-ports-retails-7-billion-problem.html; Sarah Halzack, *Why a Major Backup at West Coast Ports Could Cost the Retail Industry Billions*, WASHINGTON POST (Feb. 17, 2015) https://www.washingtonpost.com/news/wonk/wp/2015/02/17/why-a-major-backup-at-west-coast-ports-could-cost-the-retail-industry-billions/.
[33] OFFICE OF CYBER & INFRASTRUCTURE ANALYSIS, *supra* note 21, at 13.
[34] Brian McGregor, *A Reliable Waterway System is Important to Agriculture*, U.S. DEP'T OF AGRIC., AGRIC. MKTG. SERV. 1 (Oct. 2015), https://www.ams.usda.gov/sites/default/files/media/Importance%20of%20Waterways%2010-2014.pdf.
[35] *Id.* at 7.
[36] OFFICE OF CYBER & INFRASTRUCTURE ANALYSIS, *supra* note 21, at 13.

The Energy Sector still relies on foreign oil imports—in 2015, petroleum imported from foreign countries constituted approximately twenty-four percent of petroleum consumption in the U.S.[37] This corresponded to about 9.4 million barrels per day.[38] In addition, the U.S. exported approximately 4.7 million barrels per day of petroleum to other countries.[39] In 2014, fifty-five percent of all daily petroleum imports into the U.S. were through maritime shipping.[40] A cyber-attack that disrupted crude oil imports could cause a temporary increase in the instability of gasoline prices and potentially cause regional shortages (depending on the length and scope of the disruption).[41] The Chemical Sector similarly relies on imports and exports.[42] A port disruption could cause increased prices and, if a significant disruption in the chemical supply chain occurs, production of manufactured chemicals could be hampered.[43]

Goods and products are regularly offloaded from ships and transferred to other modes of transportation such as rail and truck. Thus, the impact to the transportation sector would not only be an impact to maritime transport, but would likely also affect truck and rail transport.[44] Additionally, a major port disruption could cause impacted companies to ship their goods by air freight, possibly "caus[ing] congestion within the logistic chains of air freight companies, leading to delays in the movement of goods."[45] Shipping by air freight is typically more expensive, increasing costs for the businesses and potentially negatively impacting the economy.[46]

As discussed above, the maritime industry is critical to the prosperity of the United States. However, ships not only carry "the majority of freight arriving and departing from the U.S.," they move "the bulk of critical military cargoes around the globe."[47] Thus, a maritime disruption could present a grave risk to national security. In considering the critical role that marine transportation plays, the vulnerabilities of the interconnected systems that ports and vessels rely on must also be considered.

---

[37] *Frequently Asked Questions: How much oil consumed by the United States comes from foreign countries?*, U.S. ENERGY INFO. ADMIN., http://www.eia.gov/tools/faqs/faq.cfm?id=32&t=6 (last visited Dec. 21, 2016) ("Petroleum includes crude oil and petroleum products. Petroleum products include gasoline, diesel fuel, heating oil, jet fuel, chemical feedstocks, asphalt, biofuels (ethanol and biodiesel) and other products").
[38] *Frequently Asked Questions: How much petroleum does the United States import and export?*, U.S. ENERGY INFO. ADMIN., http://www.eia.gov/tools/faqs/faq.cfm?id=727&t=6 (last visited Dec. 21, 2016).
[39] *Id.*
[40] OFFICE OF CYBER & INFRASTRUCTURE ANALYSIS, *supra* note 21, at 14.
[41] *Id.*
[42] *Id.* at 16.
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] Tiffany Hsu, *Air Freight Firms are Bustling Amid Bottlenecks at West Coast Ports*, LA TIMES (Feb. 20, 2015, 2:19 PM), http://www.latimes.com/business/la-fi-air-cargo-20150221-story.html.
[47] WALLISCHECK, *infra* note 50 at 1.

B. The Necessity of Integrated Systems in the Maritime Industry

Vessels and ports rely heavily on information systems and communications to control security, communication, navigation, cargo movement and tracking, equipment operation, and business operations.[48] Given the emerging Internet of Things (IoT), and the fact that the original concept of IoT was to improve efficiency in manufacturing,[49] it is not surprising the that the maritime industry is using similar technology. Since the typical commercial vessel spends most of its time at sea, hardwired communications and human couriers are not available to carry information. Thus, a ship truly is a "thing" in IoT parlance[50]—a typical ship contains hundreds of sensors and systems that can be remotely accessed. Such industrial control systems (ICS) are truly pervasive—"[t]hey are aboard virtually [every] ship and in the shore-side infrastructure supporting them."[51] Many of these systems are integrated to improve vessel or port efficiency.[52] While not all systems are directly connected to the Internet, their inter-connected nature leaves them vulnerable.[53] Significantly, "[f]ailure of any one of these systems can produce cascading impacts in other systems and amplify the disruption to operations."[54]

Many ICS use commercial off-the-shelf technologies that are ripe for exploitation.[55] These systems are network-based and utilize widely available communication protocols and standard operating systems.[56] Additionally, many of these systems are Internet Protocol (IP) addressable.[57] This upsurge in the usage of IP addressable devices creates significant vulnerabilities, exponentially increasing the likelihood of a severe cyber-attack.[58]

---

[48] OFF. OF CYBER & INFRASTRUCTURE ANALYSIS, *supra* note 21 at 3.
[49] Robin Kester, Note, *Demystifying the Internet of Things: Industry Impact, Standardization Problems, and Legal Considerations*, 8 ELON L. REV. 205, 206 (2016).
[50] *See Id.*
[51] Eric York Wallischeck, *ICS Security in Maritime Transportation*,, JOHN A. VOLPE NATIONAL TRANSPORTATION SYSTEMS CENTER, 1 (2013), https://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf.
[52] OFF. OF CYBER & INFRASTRUCTURE ANALYSIS, *supra* note 21 at 7.
[53] "Even limited connection to the Internet exposes control systems to all of the inherent vulnerabilities of interconnected computer networks, including viruses, worms, hackers and terrorists." WALLISCHECK, *supra* note 50 at 12.
[54] OFF. OF CYBER & INFRASTRUCTURE ANALYSIS, *supra* note 21 at 7.
[55] WALLISCHECK, *supra* note 50 at 11.
[56] *Id.*
[57] *Id.* at 12.
[58] *Id.* at 9.

C. The Gravity of the Cyber Threat

In 2013, a research team from the University of Texas at Austin successfully used a GPS spoofing device to gain control of a ship's navigation system and subtly shift an $80 million yacht off its course.[59] The yacht was tricked onto a parallel course that was several hundred meters from its intended one.[60] While the Texas team was conducting the experiment in international waters, 30 miles offshore of Italy, an attack that shifted a vessel several hundred meters off course when it was closer to land or near navigation hazards could have serious consequences.[61] Unfortunately, this is not an isolated incident. Researchers have discovered potential vulnerabilities in all transportation modes (including maritime), involving a broad range of technologies.[62]

While the highly publicized Stuxnet attack in 2010 was not directed at the maritime industry, "it is important to recognize that the same techniques used in that incident could be used to disable comparable systems used worldwide . . . including the safe and reliable movement of cargo and passengers."[63] Thankfully, the marine transportation system has not suffered a significant cyber-attack. However, major disruptions to port operations can cause wide-ranging impacts to the American economy.[64] Commentators have stated that a "broad-based cyber-attack" on the marine transportation system that slowed or halted movement of cargo, could have significant economic impact.[65] "While a cyber-attack that disables a vessel transiting the Panama Canal may only affect a single waterway, it can have significant economic impact around the globe."[66] Thus, the significant threat presented by cyber-terrorism should not be ignored.

[59] Univ. of Tex. at Austin News, *UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea* (July 29, 2013), http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea.
[60] *Id*.
[61] *Id*.
[62] WALLISCHECK, *supra* note 50 at 2.
[63] *Id*. at 14.
[64] *See supra* Section I. A.
[65] WALLISCHECK, *supra* note 50 at 2.
[66] *Id*.

II. CURRENT GOVERNMENTAL REGULATIONS AND APPROACHES

Cybersecurity is a topic that has gained significant awareness in the public consciousness.[67] Cyber-attacks are becoming more prominent and egregious in nature.[68] Much of the publicity has related to data breaches at major retailers[69] and banks,[70] but the maritime industry has occasionally gained the spotlight.[71] However, "the American public is generally unaware of . . . the impact that [Maritime Transportation System] disruptions pose to national security and economic stability. To most Americans, ships are floating hotels that travel to exotic ports . . . ."[72] This makes the risks to maritime transportation "often invisible" to the public.[73]

The United States government has continued to increase its focus on cybersecurity. President Obama recognized that "[c]yber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, implicating public and private infrastructure located in the United States and abroad."[74] Current cybersecurity regulations and laws are piecemeal but are continuing to evolve.[75]

A. *Marine Transportation*

The principal laws that cover maritime security are the Maritime Transportation Security Act and the Security and Accountability for Every Port Act.

---

[67] CHARLES BEARD ET AL, US CYBERSECURITY: PROGRESS STALLED, KEY FINDINGS FROM THE 2015 US STATE OF CYBERCRIME SURVEY 4 (2015), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-cybercrime-survey-2015.html (suggesting that "the term 'data breach' [has] become part of the broader public vernacular . . . .").

[68] *Id.*

[69] Michael Kassner, *Anatomy of the Target Data Breach: Missed opportunities and lessons learned*, ZDNET (Feb. 2, 2015, 8:29 AM), http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited Nov. 8, 2016).

[70] Portia Crowe, *JPMorgan Fell Victim to the Largest Theft of Customer Data from a Financial Institution in US History*, BUSINESS INSIDER (Nov. 10, 2015, 10:12 AM), http://www.businessinsider.com/jpmorgan-hacked-bank-breach-2015-11 (last visited Nov. 8, 2016).

[71] *See* Univ. of Tex. at Austin News, *supra* note 58.

[72] WALLISCHECK, *supra* note 50 at 2.

[73] *Id.*

[74] THE WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE/PPD-41, UNITED STATES CYBER INCIDENT COORDINATION (July 26, 2016), https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[75] Chris Laughlin, Student Note, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations are Effective*, 14 COLO. TECH. L.J. 345, 351 (2016).

1. *Maritime Transportation Security Act of 2002*

The Maritime Transportation Security Act (MTSA) was enacted in November 2002.[76] MTSA implements requirements for increased security in United States waterways, coastal areas, and ports.[77] The Act does not specifically address cybersecurity; however, it does require the development of Area Maritime Security (AMS) Plans, Vessel Security Plans, and Facility Security Plans.[78] These plans are designed to help ports, facilities, and vessels to prepare for and deter transportation security incidents.[79]

The Security and Accountability for Every Port Act (SAFE Port Act) was enacted in October 2006.[80] The Act is designed "[t]o improve maritime and cargo security through enhanced layered defenses . . . ."[81] The SAFE Port Act amended some MTSA provisions and also introduced new initiatives and programs. The latter included establishing a port security exercise program and directing the development of a strategic plan to enhance the security of the international supply chain.[82]

One critical aspect of MTSA was that it prompted the establishment of AMS Committees.[83] These committees have several key responsibilities, including identifying "critical port infrastructure and operations," identifying risks, and determining "mitigation strategies and implementation methods."[84] In addition, the committees are responsible for developing processes to continually evaluate security and assist in developing AMS Plans.[85] AMS Plans are based on the AMS Assessments that were directed by MTSA.[86]

[76] Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064 (2002).
[77] *Id.*
[78] 46 U.S.C.A. § 70103 (2010).
[79] *Id*.; 46 U.S.C.A. § 70101(6) (2006) ("The term 'transportation security incident' means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.").
[80] Security and Accountability for Every Port Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (2006).
[81] *Id*.
[82] 6 U.S.C.A. §§ 912, 941 (2016).
[83] 33 C.F.R. §§ 103.300, 103.305(a) (2016). "An AMS Committee will be composed of not less than seven members . . . who may be selected from—(1) The Federal, Territorial, or Tribal government; (2) The State government and political subdivisions thereof; (3) Local public safety, crisis management and emergency response agencies; (4) Law enforcement and security organizations; (5) Maritime industry, including labor; (6) Other port stakeholders having a special competence in maritime security; and (7) Port stakeholders affected by security practices and policies." *Id.* § 103.305(a).
[84] *Id.* § 103.310(a).
[85] *Id.* §103.310(a)(4).
[86] 46 U.S.C.A. § 70102(b) (2016) (stating that "the Secretary shall conduct a detailed vulnerability assessment of the facilities and vessels that may be involved in a transportation security incident."). These assessments shall be updated "at least every 5 years." *Id.* § 70102(b)(3). *See also* 33 C.F.R. §§ 103.400, 103.500.

AMS Assessments must: (1) identify critical port infrastructure and operations; (2) include a threat assessment identifying and evaluating potential threats; (3) include an assessment of consequences and vulnerabilities; and (4) make a security measures determination.[87] In meeting the specified elements, the assessment is to consider a number of variables including, but not limited to, physical security, security capabilities and resources, and "[r]adio and telecommunication systems, including computer systems and networks."[88] While the latter does not directly reference cybersecurity, it can be used to read the inclusion of cyber threats into MTSA. Furthermore, both Vessel Security Plans and Facility Security Plans required under MTSA must include information relating to communications and security systems.[89] Security plans must be updated every five years.[90]

A June 2014 report on maritime critical infrastructure by the Government Accountability Office (GAO) found that area maritime and facility security plans contained limited cybersecurity coverage.[91] The GAO attributed the limited coverage to the fact that the 2012 National Maritime Strategic Risk assessment developed by the Coast Guard did not address cyber risks in the maritime environment.[92] In testimony before the House Subcommittee on Border and Maritime Security, Gregory C. Wilshusen, Director of Information Security Issues for the GAO, noted that while the 2014 National Maritime Strategic Risk Assessment did identify cyber as a threat vector, it did not "fully address[] threats, vulnerabilities, and consequences of cyber incidents . . . ."[93] Director Wilshusen concluded that until this threat is more fully addressed, the "ability to appropriately plan and allocate resources for protecting maritime-related critical infrastructure" will be hindered.[94] The National Maritime Strategic Risk Assessment is conducted biennially,[95] with the next due in 2016.

[87] 33 C.F.R. § 103.405(a).
[88] *Id.* § 103.405(b)(5).
[89] *See id.* §§ 104.405, 105.405.
[90] 46 U.S.C.A. § 70103(c)(3)(G) (2016).
[91] *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity*, *supra* note 4, at 16.
[92] *Id.* (the 2012 assessment was the most current available at the time of the report).
[93] *DHS Needs to Enhance Efforts to Address Port Cybersecurity: Hearing on Maritime Critical Infrastructure Protection Before the H. Subcomm. on Border and Maritime Security, H. Comm. on Homeland Security*, 114th Cong. 7 (2015) (statement of Gregory C. Wilshusen, Dir., Info. Security Issues, Gov't Accountability Off.).
[94] *Id.*
[95] *Id.* at 6.

2. *Port Security Grant Program*

MTSA also introduced the Port Security Grant Program (PSGP)[96] to help ports with funding for the security requirements it mandated.[97] The Federal Emergency Management Agency (FEMA) administers the program and consults with the U.S. Coast Guard, among others, to make award decisions.[98] The grant program was designed to allocate funds based on risk.[99]

The fiscal year (FY) 2014 PSGP Funding Opportunity Announcement (FOA) allowed applicants to request funding for cybersecurity vulnerability assessments.[100] Vulnerability assessments had not been something typically funded under PSGP; however, the FOA noted that "considering the relative newness of Cybersecurity as a priority within the program and the need to develop and enhance the voluntary Cybersecurity Framework, vulnerability assessments may be funded as contracted costs."[101] The FY 2014 PSGP also stated that cybersecurity was one of the funding focus areas.[102] FY 2014 was only the second year that cyber was considered a major funding priority.[103] Cybersecurity remained an identified funding priority in 2015 and 2016.[104]

[96] 46 U.S.C.A. § 70107 (2016).
[97] Commander Joseph Kramek, *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities*, CTR. FOR 21ST CENTURY SEC. AND INTELLIGENCE 9 (July 2013), https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf.
[98] *Id*.
[99] 46 U.S.C.A. § 70107(a) (2016) ("In administering the grant program, the Secretary shall take into account national economic, energy, and strategic defense concerns based upon the most current risk assessments available.").
[100] *Funding Opportunity Announcement: FY 2014 Port Security Grant Program*, FED. EMERGENCY MGMT. AGENCY 38 (2014), https://www.fema.gov/media-library-data/1396623742630-9e497a99bef3e3c0265bbf84993b5e69/FY_2014_PSGP_FOA_Final_Revised.pdf.
[101] *Id*.
[102] *FY 2014 Port Security Grant Program Fact Sheet*, FED. EMERGENCY MGMT. AGENCY 2 (2014), https://www.fema.gov/media-library-data/1406300857129-09e62587b8f79e748c585e37cdba09a9/PSGP_Fact%20Sheet_Final.pdf.
[103] Looking back as far as 2005, 2013 was the first year that cyber was specifically called out as a major funding priority. *See generally Port Security Grant Program*, FED. EMERGENCY MGMT. AGENCY, https://www.fema.gov/port-security-grant-program (last visited Mar. 27, 2017) (wherein FY 2005 data is the earliest available on the FEMA PSGP website).
[104] *FY 2015 Port Security Grant Program Fact Sheet*, FED. EMERGENCY MGMT. AGENCY 2 (2015), https://www.fema.gov/media-library-data/1438021685566-9cf51877eec3f17c6495b672334eb050/FY_2015_PSGP_Fact_Sheet_Allocations.pdf; *FY 2016 Port Security Grant Program Fact Sheet*, FED. EMERGENCY MGMT. AGENCY, 2 (2016), https://www.fema.gov/media-library-data/1467237017233-ba181560021a43339f4c3e0253212671/FY_2016_PSGP_Fact_Sheet_Final.pdf.

However, while cybersecurity was identified as a funding priority in 2014, the national review panel for grants did not reach out to any cyber subject matter experts to assist it in making decisions about which cyber-related grants were most worthy of funding.[105] For the 2015 grants, FEMA did report that "they have consulted with the Coast Guard's Cyber Command on high-dollar-value cyber projects and that Cyber Command officials sat on the review panel for one day to review several other cyber projects."[106] However, FEMA provided no formal written guidelines to ensure that grant reviewers consulted appropriate cyber expertise in either the field (captain of the port) level or national level review process.[107] The FY 2016 Notice of Funding Opportunity (NOFO) did contain a more detailed discussion of cybersecurity than previous years, however, it still did not require that grant reviewers consult cyber professionals when reviewing cyber projects.[108]

B. *Critical Infrastructure*

The National Infrastructure Protection Plan (NIPP) lays the foundation for private sector and government entities in the critical infrastructure community to work together to ensure critical infrastructure safety and resilience through proper risk management practices.[109] NIPP advocates an approach through public-private partnership, ensuring that all stakeholders in the critical infrastructure community are represented.[110] The 2013 NIPP update is consistent with Executive Order 13636, "Improving Critical Infrastructure Cybersecurity,"[111] and Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience."[112]

---

[105] *DHS Needs to Enhance Efforts to Address Port Cybersecurity*, *supra* note 92, at 9.
[106] *Id.*
[107] *Id.*
[108] *Notice of Funding Opportunity: FY 2016 Port Security Grant Program*, FED. EMERGENCY MGMT. AGENCY 40 (2016), https://www.fema.gov/media-library-data/1455573875236-07ce03a778118ecc2ead8e1aae84185e/FY_2016_PSGP_NOFO_FINAL.pdf.
[109] *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, U.S. DEP'T OF HOMELAND SEC. 1–2 (2013), https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.
[110] *Id.* at 3.
[111] Exec. Order No. 13,636, *infra* note 112.
[112] *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, *supra* note 108; Presidential Policy Directive/PPD-21, *supra* note 22.

1. *Executive Order 13636 and Presidential Policy Directive 21*

In February 2013, President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[113] This order recognized that "[t]he cyber threat to critical infrastructure . . . represents one of the most serious national security challenges we must confront."[114] It defined critical infrastructure broadly: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[115] Arguably maritime critical infrastructure is covered under this definition.

Executive Order 13636 stated that "[i]t is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[116] The Order promoted partnership between the government and the private sector, and sought to create an information sharing program that allowed for more timely sharing of information between the government and the private sector.[117] In addition, the Order directed all agencies to ensure that civil liberties and privacy protections were considered and incorporated into any cyber-related activities.[118]

On the same day that Executive Order 13636 was issued, President Obama also published Presidential Policy Directive Twenty-One (PPD-21), "Critical Infrastructure Security and Resilience."[119] The sixteen critical infrastructure sectors recognized by PPD-21 were each assigned a Federal Sector Specific Agency to lead the federal efforts.[120] PPD-21 focused on both the cyber and physical sides of critical infrastructure, and recognized the interconnected nature of infrastructure systems.[121]

---

[113] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).
[114] *Id.* § 1.
[115] *Id.* § 2.
[116] *Id.* § 1.
[117] *Id.* § 4.
[118] *Id.* § 5.
[119] *Critical Infrastructure Security and Resilience*, *supra* note 22.
[120] *Id.* ("The term 'Sector-Specific Agency' (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise . . . .").
[121] *Id.*

PPD-21 set three strategic imperatives to shape the Federal government approach.[122] The first imperative directs implementation of a "national unity of effort," designed to increase situational awareness and clarify relationships between public and private stakeholders.[123] The second imperative focuses on ensuring efficient information exchange, both within the government and with the operators and owners of critical infrastructure.[124] Like Executive Order 13636, PPD-21 stresses that information sharing "must be done while respecting privacy and civil liberties."[125] The final strategic imperative focuses on an "integration and analysis function," and seeks to use this function to inform both planning and operational decision making.[126]

2. *National Institute of Standards and Technology Cybersecurity Framework*

Executive Order 13636 also directed the National Institute of Standards and Technology (NIST) "to lead the development of a framework to reduce cyber risks to critical infrastructure."[127] The order directed that "[t]he Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[128]

The NIST Framework was promulgated on February 12, 2014, one year to the day after Executive Order 13636.[129] The Framework was collaboratively developed by both governmental and private sector entities and identified "a set of industry standards and best practices . . . ."[130] Use of the Framework is voluntary and it is designed to complement, rather than replace, existing processes and programs.[131] The Framework is broken down into "three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles."[132]

---

[122] *Id.*
[123] *Id.*
[124] *Critical Infrastructure Security and Resilience*, *supra* note 22. "(2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government;…"
[125] *Id. see also*, Exec. Order No. 13636, *supra* note 112 at § 5(a).
[126] Presidential Policy Directive/PPD-21, *supra* note 22. NOTE: maybe use quote, "(3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure."
[127] Exec. Order No. 13636, *supra* note 112, at § 7(a).
[128] *Id.*
[129] NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (last visited April 20, 2017).
[130] *Id*. at 1.
[131] *Id*. at 4.
[132] *Id.*

The Framework Core is based on five functions that are concurrent and should be continuously considered.[133] The functions are "Identify, Protect, Detect, Respond, [and] Recover,"[134] and are designed to represent a strategic, birds-eye ("high-level") view of cybersecurity risk.[135] The functions are further broken down into categories (functional groups)[136] and subcategories[137] (specific outcomes). In addition, informative references are given for each subcategory, capturing common practices used to achieve desired outcomes.[138]

The Framework Implementation Tiers are designed to reflect the level at which an entities' cybersecurity practices correspond to the risk management procedures described in the Framework.[139] The Tiers cover a range that moves from a more informal and reactive response, to responses that are adaptive and "risk-informed."[140] The Tiers help "provide context on how an organization views cybersecurity risk and the processes in place to manage that risk."[141] In order to determine the most appropriate Tier to mitigate risk and feasibly meet organizational goals, each organization should consider their unique constraints, objectives, threat environment, and legal or regulatory requirements.[142]

The Framework Profiles are the outcomes that organizations select from the Framework categories and subcategories based on their individual needs.[143] A Profile can be particularly helpful in examining an organization's current cybersecurity posture (i.e. "as is") and comparing it with a target Profile (i.e. hope "to be").[144] This comparison can help an organization identify steps that need to be taken to reach cybersecurity protection goals.[145] Organizations can have multiple Profiles, each aligned with particular cyber vulnerable business components and recognizing particular organizational needs.[146]

---

[133] *Id.*
[134] NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (last visited April 20, 2017).
[135] *Id.* at 4.
[136] *Id.* at 7, 19 (Figure 1 (p. 7) and Table 1 (p. 19)).
[137] *Id.* at 8. "Subcategories further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category."
[138] *Id.*
[139] NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 5 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (last visited April 20, 2017).
[140] *Id.* at 5, 10 (the Tier definitions are: Tier 1 (Partial), Tier 2 (Risk Informed), Tier 3 (Repeatable), Tier 4 (Adaptive)).
[141] *Id.* at 9.
[142] *Id.*
[143] *Id.* at 5.
[144] NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 5 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (last visited April 20, 2017).
[145] *Id.* at 11.
[146] *Id.*

The NIST Framework is a good starting point to strengthen cybersecurity programs. Additional standards developed collaboratively between the private sector and government should be encouraged. These additional standards could build on this initial Framework, adding to the depth and breadth of cybersecurity knowledge and showcasing best practices and procedures. Such additional collaborative products would benefit both the government and industry, helping maintain the security and resiliency of American critical infrastructure. The maritime industry has recognized the importance of the NIST Framework—all of the recently promulgated industry guidance cite the Framework and suggest incorporating many of its recommended practices.[147]

3. *United States Coast Guard Cyber Strategy*

Partially due to Executive Order 13636, the United States Coast Guard promulgated a Cyber Strategy in 2015.[148] This Strategy designates infrastructure protection as one of the Coast Guard's strategic priorities in the cyber domain.[149] It identifies two goals and four strategies to help address cyber risks to maritime critical infrastructure.[150] Additionally, in 2013, the Coast Guard created a Cyber Command to coordinate its cybersecurity efforts.[151]

The first goal of the strategy is the promotion of cyber risk awareness and management through risk assessment.[152] This goal has two objectives: 1) "Improve Port-Wide Cybersecurity Risk Assessment Tools and Methodologies," and 2) "Improve Cybersecurity Information Sharing."[153] To achieve these objectives, the Coast Guard will seek to leverage currently existing cybersecurity risk assessment tools, including those currently employed by the Coast Guard, and those employed by other agencies and industries.[154] It will also take steps to establish information sharing protocols and work with industry partners and other government agencies to facilitate information sharing across critical infrastructure sectors.[155]

[147] *See supra* Section III.
[148] U.S. COAST GUARD, *supra* note 19, at 5.
[149] *Id.* at 31.
[150] *Id.* at 32-33.
[151] *Id.* at 7.
[152] *Id.* at 32 ("The Coast Guard will incorporate cybersecurity into aspects of maritime operations in order to reduce the risk . . . and to continue to protect the nation's maritime critical infrastructure and the American people.").
[153] U.S. COAST GUARD, *supra* note 19, at 32.
[154] *Id.*
[155] *Id.*

The second goal is aimed at prevention and seeks to "Reduce Cybersecurity Vulnerabilities."[156] This goal also has two objectives: 1) "Reduce Cyber Vulnerability for Vessels and Facilities," and 2) "Incorporate Cybersecurity into Training and Education Requirements."[157] These objectives target development of guidance and education by working with industry partners, including international organizations, to determine best practices and protocols.[158]

C. *Recent Cybersecurity Legislation*

1. *2014 Cybersecurity Legislation*

Prior to December 2014, no cybersecurity laws had been enacted since the Federal Information Security Management Act of 2002.[159] In December 2014, however, Congress approved five Acts related to cybersecurity.[160] The legislation most closely related to critical infrastructure and marine transportation are the National Cybersecurity Protection Act of 2014 and the Cybersecurity Enforcement Act of 2014.

[156] *Id.* at 33 ("Understanding the vulnerabilities associated with cyber systems enables the Coast Guard and the marine industry to take appropriate steps to reduce the risk to maritime cyber critical infrastructure from attack, exploitation, failure, or misuse.").
[157] *Id.*
[158] U.S. COAST GUARD, *supra* note 19, at 33.
[159] Lawrence J. Trautman, Article, *Cybersecurity: What About U.S. Policy?*, 2015 U. Ill. J.L. Tech. & Pol'y 341, 344 (2015).
[160] *Id.* (these include the National Cybersecurity Protection Act of 2014, the Federal Information Security Modernization Act of 2014, the Cybersecurity Workforce Assessment Act, the Homeland Security Workforce Assessment Act, and the Cybersecurity Enhancement Act of 2014).

a. National Cybersecurity Protection Act of 2014

The National Cybersecurity Protection Act of 2014 amends the Homeland Security Act of 2002, adding a provision for a National Cybersecurity and Communications Integration Center (NCCIC).[161] According to the Department of Homeland Security, NCCIC "is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement."[162] The mission of NCCIC is to decrease the severity and likelihood of events that may cause considerable compromise to the resilience and security of key national communications and information technology networks.[163]

A recent policy letter released by the Coast Guard regarding MTSA regulated facilities and vessels allows certain cyber incidents to be reported to the NCCIC.[164] The policy included cyber incidents in the definitions of reportable breaches of security and suspicious activity.[165] It was also noted that "[p]lausible terrorist attack scenarios include combined cyber and physical incidents."[166] Once a cyber incident is reported, "the NCCIC may be able to provide technical assistance to the porting party."[167]

In addition to establishing the NCCIC, the Cybersecurity Protection Act contains a number of provisions addressing information sharing and required reports.[168] Furthermore, for the critical infrastructure sector, it requires the DHS under Secretary for Critical Infrastructure Protection and Cybersecurity to "develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks . . . to critical infrastructure."[169] These plans are to be developed in coordination with appropriate Federal, State, local, and industry partners.[170]

[161] Nat'l Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (2014).
[162] *National Cybersecurity & Communications Integration Center*, U.S. DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center (last visited Dec. 22, 2016).
[163] *Id.*
[164] U.S. Coast Guard, Policy Letter on Reporting Suspicious Activity & Breaches of Security (Dec. 14, 2016), https://homeport.uscg.mil (click on "Maritime Security" on the left menu bar and then "Policy." This letter is listed as "CG-5P Policy Ltr No. 08-16, Reporting Suspicious Activity & Breaches of Security") (Transportation Security Incidents are normally reported to the National Response Center. However, "cyber incidents that do not also involve physical or pollution effects" may now be reported "to the NCIC in lieu of the NRC . . . .").
[165] *Id.* at ¶ 3.A & B.
[166] *Id.* at ¶ 2.D.
[167] *Id.* at ¶ 3.C.iii.
[168] Nat'l Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (2014).
[169] *Id.* at § 7.
[170] *Id.*

b. Cybersecurity Enhancement Act of 2014

The Cybersecurity Enhancement Act of 2014 is "An Act to provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes."[171] Title I of the Act amends the National Institute of Standards and Technology Act (15 U.S.C. 272), adding provisions that strengthen public-private collaboration in the cybersecurity realm, including "on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards . . . to cost-effectively reduce cyber risks to critical infrastructure."[172]

Title II of the act focuses on cybersecurity research and development.[173] Among other provisions, it directs the development of a federal cybersecurity research and development strategic plan that is to be updated every four years and be "based on an assessment of cybersecurity risk to guide the overall direction of Federal cybersecurity and information assurance research and development . . . ."[174] While this strategic plan is to guide Federal cybersecurity research, in developing and updating the plan, the government entities are to work closely with the private sector, including academia, industry, and interested stakeholders.[175] This will allow the government to solicit recommendations and ensure that Federal research is not duplicating current private sector plans.[176]

Title III of the Act involves education and workforce development.[177] This portion of the Act promotes challenges and competitions to stimulate cybersecurity innovation and learning.[178] It also codifies a scholarship-for-service program designed to train and recruit promising individuals to fulfil cybersecurity positions at the tribal, local, State, and Federal levels.[179] Title IV, Cybersecurity Awareness and Preparedness, involves education.[180] Specifically, it orders the NIST Director, in consultation with other appropriate agencies and stakeholders, "to coordinate a national cybersecurity awareness and education program . . . ."[181]

Title V, Advancement of Cybersecurity Technical Standards, directs NIST to ensure coordination between agencies developing international technical information system security standards, to develop a cloud computing strategy for the Federal Government, and to support identity management research and development.[182] In the first two tasks, NIST is explicitly directed to consult with "other relevant Federal agencies and stakeholders from the private sector."[183]

---

[171] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).
[172] *Id.* at § 101(a).
[173] *Id.* at § 201.
[174] *Id.* at § 201(a)(1).
[175] *Id.* at § 201(a)(2)(B).
[176] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 § 201(a)(2)(B) (2014).
[177] *Id.* at §§ 301-302.
[178] *Id.* at § 301.
[179] *Id.* at § 302.
[180] *Id.* at § 401.
[181] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 § 401(a). (2014).
[182] *Id.* at §§ 501-504.
[183] *Id.* at §§ 502-503.

2. *Cybersecurity Act of 2015 and Recent Presidential Policy*

Information sharing has been one of the most consistently contentious issues across the cyber domain.[184] Obstacles that have hindered information exchange include: the concerns that shared information could be used as evidence of failing to meet a regulatory standard, that after being shared with the government such information might be available to the public through a public records request, and concern over individual privacy rights.[185] The Cybersecurity Act of 2015 seeks to "facilitate and promote" timely information sharing across Federal and non-Federal entities to encourage sharing of information about cyber threats.[186]

a. Cybersecurity Act of 2015

The majority of the Cybersecurity Act is focused on information sharing.[187] It requires the Departments of Justice and Homeland Security to develop procedures to promote timely sharing of cyber information.[188] The Act also provides some key protections to private sector entities that share cybersecurity information.[189] It exempts information from disclosure via the Freedom of Information Act and requires that entities sharing information remove material that identifies specific individuals.[190] Additionally, the Act limits how federal, state, tribal, and local governments can use the information.[191] It specifically states that information "shared with a State, tribal, or local government . . . shall not be used . . . to regulate, including an enforcement action, the lawful activity of any non-Federal entity."[192] The federal government may only use the information for a limited number of purposes, including "a cybersecurity purpose,"[193] identifying cybersecurity vulnerabilities or threats, or a purpose related to other specified threats.[194] Additionally, the Act includes an entire section on "Protection from liability."[195] Legal commentators have suggested that such liability protection is a significant incentive to share information.[196] The Act specifically states that "[n]o cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed . . ." for information shared in accordance with the Act.[197]

---

[184] Peter Carey et al., *President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing*, NAT'L L. REV., (January 3, 2016).
[185] *Id.*
[186] 6 U.S.C.A. § 1502 (2015).
[187] Peter Carey et al., *supra* note 182.
[188] 6 U.S.C.A. § 1502 (2015).
[189] Peter Carey et al., *supra* note 182.
[190] 6 U.S.C.A. § 1503 (2015).
[191] 6 U.S.C.A. §§ 1503, 1504 (2015).
[192] 6 U.S.C.A. § 1503(4)(C) (2015).
[193] 6 U.S.C.A. § 1501 (2015) ("The term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.").
[194] 6 U.S.C.A. § 1504(5)(A) (2015) (the other threats include death, serious bodily or economic harm, terrorist acts, "a serious threat to a minor," fraud or identify theft, espionage, or trade secret protection).
[195] 6 U.S.C.A. § 1505 (2015).
[196] Peter Carey et al, *supra* note 182.
[197] 6 U.S.C.A. § 1505(a), (b) (2015).

b. 2016 Presidential Policy

In February 2016, President Obama signed Executive Order 13718, creating a Commission on Enhancing National Cybersecurity under the Department of Commerce.[198] The Commission was made up of twelve members and included former government officials as well as representatives from academia and industry.[199] Executive Order 13718 directed the Commission to compile a report that included "detailed recommendations to strengthen cybersecurity in both the public and private sectors . . . ."[200]

The report was completed on December 1, 2016, and highlighted the critical need for partnerships between the private and public sectors.[201] The report identified six "major imperatives" which were further broken down into sixteen recommendations and fifty-three action items.[202] The Commission felt "that most recommendations can and should begin in the near term, with many meriting action within the first 100 days of the new Administration."[203] The aim of the report was to make recommendations for actions that can be incorporated during the next decade to help increase cybersecurity in both the private and public sectors.[204]

[198] Exec. Order No. 13718, 81 Fed. Reg. 29 (Feb. 9, 2016).
[199] *Comm'n on Enhancing Nat'l Cybersecurity*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/cybercommission (last visited Jan. 23, 2017).
[200] Exec. Order No. 13718, *supra* note 197 at § 3.
[201] COMM'N ON ENHANCING NAT'L CYBERSECURITY, REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY (Dec. 1, 2016), https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.
[202] *Id.* at 2 ("The imperatives are: 1. Protect, defend, and secure today's information infrastructure and digital networks. 2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy. 3. Prepare consumers to thrive in a digital age. 4. Build cybersecurity workforce capabilities. 5. Better equip government to function effectively and securely in the digital age. 6. Ensure an open, fair, competitive, and secure global digital economy.").
[203] *Id.*
[204] Exec. Order No. 13718, *supra* note 196, § 3. R4.1

The introduction to Presidential Policy Directive 41 (PPD-41), "United States Cyber Incident Coordination," notes that U.S. infrastructure "is vulnerable to malicious activity, malfunction, human error, and acts of nature, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency . . . ."[205] PPD-41 highlights the shared responsibility of government, private sector, and individual stakeholders.[206] Further, it delineates principles under which the Federal Government are to respond to cyber incidents (involving either private sector or government entities).[207] For what the PPD termed "significant cyber incidents,"[208] lead Federal agencies were designated "and an architecture for coordinating the broader Federal Government response" was established.[209] PPD-41 mandated coordinated and "concurrent lines of effort" by federal agencies.[210] The "concurrent lines of effort" are divided into four areas of response, three undertaken for all cyber incidents, and the fourth only when a federal government agency is the affected party.[211] The first three areas are "threat response; asset response; and intelligence support and related activities."[212] The final response area is "to manage the effects of the cyber incident on [the affected federal agency's] operations, customers, and workforce."[213]

Threat response is focused on investigation, collecting evidence and intelligence, working to link related incidents, mitigation of any immediate threats, and other related tasks.[214] Another goal is to "facilitat[e] information sharing and operational coordination with asset response."[215] Asset response provides technical assistance to the parties affected by cyber incidents, to help them "protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents . . . ."[216] Additionally, this area of response looks beyond the immediate threat vector to consider other entities and areas that may be vulnerable.[217] Asset responders also assist by "providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery."[218] The threat and asset response areas are designed to be closely related and enhance communications and information sharing.[219] The intelligence support activity focuses on building situational awareness, analyzing threats, identifying gaps, and gaining the ability to mitigate or degrade adversarial threat capabilities.[220]

---

[205] Presidential Policy Directive/PPD-41, *supra* note 73.
[206] *Id.*
[207] *Id.*
[208] *Id.* § II.B ("Significant cyber incident. A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.").
[209] Presidential Policy Directive/PPD-41 § I, *supra* note 73.
[210] *Id.* § IV.
[211] Presidential Policy Directive/PPD-41, *supra* note 73, § IV.
[212] *Id.*
[213] *Id.*
[214] *Id.* § IV.A.
[215] Presidential Policy Directive/PPD-41, *supra* note 73, § IV.B.
[216] *Id.*
[217] *Id.*
[218] *Id.*
[219] *Id.*
[220] *Id.* at § IV.C. R4.1.

When a federal agency is an affected party, efforts will be taken to manage the effects of the incident.[221] This "line of effort" will be managed by the affected agency and will include broad-ranging efforts, from external affairs to ensuring operational continuity.[222] When a private entity is the affected party, the government will not play an active role in managing the effects of the incident, "but it will remain cognizant of the affected entity's response activities . . . ."[223] For private sector entities, the most relevant government agency will generally be responsible for maintaining this awareness.[224]

Given the shared responsibility held by both the government and private sector, it is also important for the private sector to cultivate situational awareness and develop threat response procedures. Developing industry guidelines and procedures is an effective way to share best practices and lessons learned. Such guidelines should be shared across company lines and with the government so that all industry partners can benefit from the information.

[221] Presidential Policy Directive/PPD-41, *supra* note 73, § IV.D.
[222] *Id.*
[223] *Id.*
[224] *Id.*

III. MARITIME INDUSTRY PRACTICE AND GUIDANCE

The maritime industry has recently taken an increased notice of cyber risk. Three industry-leading organizations promulgated guidance in 2016 alone. These guidelines and suggestions highlight best practices and approaches to address maritime cyber risk management. While differing in scope, some basic principles emerge that are consistent throughout the guidelines. All three advocate integrating the NIST Framework principles into the industry's cyber approaches. Additionally, increasing cyber awareness was recognized as a critical step in improving cybersecurity. While the American Bureau of Shipping Guidance Notes are by far the most thorough, each of the industry guidelines bring an important perspective to the table. These guidelines are important, not so much for the techniques and procedures they discuss, but for the fact that these highly influential maritime organizations are taking notice of the cyber threat and working to increase industry awareness.

A. *Baltic and International Maritime Council: The Guidelines on Cyber Security Onboard Ships*

"The Guidelines on Cyber Security Onboard Ships," released by the Baltic and International Maritime Council (BIMCO) and several other influential maritime associations, is tailored to ship-owners and operators.[225] The Guidelines are designed to give pointers on assessing operations and implementing the necessary actions and procedures to maintain cybersecurity aboard ships.[226] The "Guidelines focus on the unique issues facing the shipping industry onboard ships."[227] Additionally, the Guidelines aim to improve awareness and understanding of good cybersecurity practices.[228]

[225] BALTIC & INT'L MAR. COUNCIL, THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS 1 (Version 1.1, 2016), https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf.
[226] *Id.*
[227] *Id.*
[228] *Id.*

The Guidelines set out a framework for cybersecurity awareness that includes six related steps: identify threats; identify vulnerabilities; assess risk exposure; develop protection and detection measures; establish contingency plans; and respond to cyber security incidents.[229] To identify threats, a ship owner or operator must understand both the external and internal[230] threat possibilities.[231] While cyber risk is pervasive, each maritime entity needs to identify the specific risks to their operation, company, trade, or vessel.[232] In identifying vulnerabilities, companies need to cultivate awareness "of any specific aspect of their operations that might increase their vulnerability to cyber incidents."[233] Additionally, the Guidelines point out that each entity must have knowledge and understanding of any protection measures already in place and the capabilities and limitations of these measures.[234]

In assessing risk exposure, the Guidelines specify that any cyber protections already in place, along with the specific vulnerabilities that are found in the maritime industry, should be considered.[235] The maritime realm presents a number of features that are potentially vulnerable to cyber threats. "Multiple stakeholders are often involved in the operation and chartering of a ship potentially resulting in lack of accountability for the IT infrastructure."[236] Additionally, ships regularly "interface[] with other parts of the global supply chain . . . [and share information] with shore-based service providers."[237] Furthermore, many ship systems, including those related to environmental protection and safety, are controlled by computers.[238] The Guidelines suggest using the NIST framework to assess current approaches and help identify risks.[239] It is additionally suggested that each company should conduct an internal risk assessment to identify potential threats and survey current systems and procedures.[240] This self-assessment should be followed up by a third-party assessment to find any additional threat vectors missed during the self-assessment.[241]

---

[229] *Id.* at 2.
[230] *Id.*
[231] BALTIC & INT'L MAR. COUNCIL, THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS 1 (Version 1.1, 2016), https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf. (Internal threat possibilities are caused by insufficient awareness or inappropriate use).
[232] *Id.* at 3.
[233] *Id.*
[234] *Id.* at 2.
[235] *Id.* at 6.
[236] *Id.*
[237] BALTIC & INT'L MAR. COUNCIL, THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS 1 (Version 1.1, 2016), https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf. at 6.
[238] *Id.*
[239] *Id.*
[240] *Id.* at 7.
[241] *Id.* at 10.

Reducing risk through the development of protection and detection measures is one of the most important steps in the cybersecurity awareness cycle. The Guidelines suggest implementing a layered approach that focuses on both technical and procedural defenses.[242] Technical defenses are "focused on ensuring that onboard systems are designed and configured to be resilient to cyber-attacks."[243] Procedural defenses ensure that company policies, procedures (both safety and security), and access controls cover cyber vulnerabilities.[244] One critical procedural control identified by the Guidelines is ensuring adequate training and awareness of personnel who operate and support the ship.[245]

Each company should establish "appropriate contingency plans in order to effectively respond to cyber incidents."[246] These plans should be periodically tested so that personnel are familiar with the appropriate procedures to follow in the case of a cyber incident.[247] The Guidelines further suggest that these plans should be available in some type of non-electronic form in case the cyber incident involves deleting or disrupting access to data.[248]

According to the Guidelines, the final step, "respond to cyber security incidents," should be informed by all the previous steps in the awareness cycle.[249] Furthermore, the plans that were developed should be implemented, and their effectiveness measured.[250] The Guidelines also specify that vulnerabilities and threats should be re-evaluated in light of the actual incident.[251]

[242] *Id.* at 12.
[243] BALTIC & INT'L MAR. COUNCIL, THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS 1 (Version 1.1, 2016), https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf.
[244] *Id.*
[245] *Id.* at 15.
[246] *Id.* at 18.
[247] *Id.*
[248] *Id.*
[249] BALTIC & INT'L MAR. COUNCIL, THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS 1 (Version 1.1, 2016), https://www.marad.dot.gov/wp-content/uploads/pdf/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016.pdf.
[250] *Id.*
[251] *Id.*

B. *International Maritime Organization: Interim Guidelines on Maritime Cyber Risk Management*

The Maritime Safety Committee of the International Maritime Organization (IMO) approved and published "Interim Guidelines on Maritime Cyber Risk Management" in June 2016.[252] The Committee's reason for releasing the Guidelines was "the urgent need to raise awareness on cyber risk threats and vulnerabilities."[253] This short document gives a broad overview of items to consider related to cyber risk and references both the NIST Framework and the BIMCO Guidelines.[254] The IMO Guidelines focus on a risk management approach and are designed to be incorporated with existing industry processes and procedures.[255]

The Guidelines advocate creating a culture of cyber risk awareness that starts at the most senior level of management and flows throughout every level of an organization.[256] In order to create and sustain this culture of risk awareness, the Guidelines focus on the same five functional elements identified in the NIST framework: identify, protect, detect, respond, and recover.[257] The Guidelines note that the "functional elements are not sequential—all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework."[258]

The "identify" element contains a suggestion that all personnel responsibilities and roles related to cybersecurity should be identified.[259] Additionally, any critical data, capabilities, assets or systems that are potential vulnerable to cyber-attack should also be identified.[260] Under "protect," IMO advocates implementing risk control measures and processes that focus on protecting against a potential cyber event, and aim to ensure operational continuity in the face of such an event.[261] The "detect," "respond," and "recover" elements focus on developing and implementing processes that effectively allow organizations to detect a cyber event, and respond in such a way that allows for timely restoral and recovery of critical systems.[262]

---

[252] INT'L MAR. ORG., INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT, MSC.1/CIRC. 1526 (2016), https://www.marad.dot.gov/wp-content/uploads/pdf/MSC.1-Circ.1526-Interim-Guidelines-On-Maritime-Cyber-Risk-Management-....pdf.
[253] *Id.*
[254] *Id.* at 4.
[255] *Id.* at 1.
[256] *Id.* at 3.
[257] *Id.*
[258] INT'L MAR. ORG., *supra* note 250 at 3.
[259] *Id.*
[260] *Id.*
[261] *Id.*
[262] *Id.*

C. *American Bureau of Shipping CyberSafety™ Guidance Notes*

In 2016, the American Bureau of Shipping (ABS)[263] released a series of five volumes of CyberSafety™ Guidance Notes. This series is by far the most detailed guidance available for maritime cybersecurity. In the Foreword to the second volume of the series, ABS notes that "[e]xposure to these [cyber] threats has become pervasive due to the exponential growth of automation methods—and increasingly, autonomy—that has penetrated nearly all aspects of shipboard and offshore asset systems."[264] ABS points out that since such systems are integral to multiple facets of platform, ship, or asset operations, they are critical to operational safety and security.[265]

Volume 1: *Cybersecurity*, published in February 2016, offers cybersecurity commentary and best practices.[266] Cyber awareness should be "a foundational element of overall safety and security within and across the marine and offshore communities."[267] The volume is divided into five sections. The first two sections are more general in nature, discussing cybersecurity and giving advice on developing a cybersecurity program. The last three sections gather best practices that apply to marine and offshore operations. In discussing best practices, ABS advocates have developed nine basic capabilities as the foundation of a successful cybersecurity program.[268] Once the baseline capabilities are established, additional capabilities should be developed to provide increasing breadth and depth to a cybersecurity program.[269]

---

[263] ABS is an internationally recognized classification society. A classification society is "an organization that develops official standards for the shipping industry and checks the condition of ships and their equipment to make certain they are safe and meet the official standards of the shipping industry." *Classification Society*, CAMBRIDGE BUSINESS ENGLISH DICTIONARY, http://dictionary.cambridge.org/us/dictionary/english/classification-society (last visited Mar. 28, 2017).

[264] American Bureau of Shipping, *Guide for: Cybersecurity Implementation for the Marine and Offshore Industries*, 2 ABS CYBERSAFETY™ ii (2016), http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251_cybersafetyV2/CyberSafety_V2_Cybersecurity_Guide_e.pdf.

[265] *Id.*

[266] American Bureau of Shipping, *Guidance Notes on: the Application of Cybersecurity Principles to Marine And Offshore Operations*, 1 ABS CYBERSAFETY™ ii (2016), http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf.

[267] *Id.* at ii.

[268] *Id.* at Fig. 1 (the basic capabilities are: "1-Exercise Best Practices; 2-Build the Security Organization; 3-Provision for Employee Awareness & Training; 4-Perform Risk Assessment; 5-Provide Perimeter Defense; 6-Prepare for Incident Response & Recovery; 7-Provide Physical Security; 8-Execute Access Management; and 9-Maintain Asset Management").

[269] *Id.* at 5.

Volume 2, published in September 2016,[270] establishes criteria to assess the readiness of assets and systems to prevent cyber incidents that could compromise the security and/or safety of assets, systems, and critical data.[271] This volume, referred to as a Guide, "provides a model for implementing cybersecurity programs."[272] A ship under the classification purview of ABS that complies with the criteria and procedures identified in the Guide can be issued a "CyberSafety Management System Certificate (CMSC) and Notation . . . ."[273] Additionally, a facility can be issued a "Certificate of Cyber Compliance (CCC)."[274] The Guide lays out detailed procedures and processes for obtaining and maintaining certification.[275]

Volume 3 is specifically focused on "data integrity."[276] This particular Guidance Note "is intended to help the industry realize the new benefits from data sources and data analytics systems via implementation of Data Integrity concepts."[277] The Note focuses on three main areas: characterizing data, securing data, and maintaining data integrity.[278]

[270] Volumes 2–5 were all published in September 2016.
[271] *See* American Bureau of Shipping, *supra* note 263 at ii.
[272] *Id.* at 1.
[273] *Id.* (Vessels or "offshore assets not classed by ABS can be issued a 'Statement of Fact' when they are in conformance with the requirements of this Guide.").
[274] *Id.*
[275] *Id.* at 2–4.
[276] American Bureau of Shipping, *Guidance Notes on: Data Integrity for Marine and Offshore Operations*, 3 ABS CYBERSAFETY™ ii (2016), http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/252_cybersafetyV3/CyberSafety_V3_Data_Integrity_GN_e.pdf.
[277] *Id.*
[278] *Id.* at 3.

Volume 4, the *Guide for Software Systems Verification*, is focused on the software component of the control systems found onboard vessels (and offshore assets).[279] "The objective of this Guide is to reduce software-related incidents that could negatively affect the security, safety and performance of [computer-based control] systems."[280] The Guide presents various criteria and processes designed to verify the software portion of vessel control systems.[281] ABS suggests that the "verification and validation organization" (used to perform software verification) should be a completely independent third-party.[282] Systems identified as of particular note include dynamic positioning, power management, thruster control, and blowout prevention.[283] This Guide focuses exclusively on software and does not provide procedures to verify hardware.[284] A vessel that conforms to the criteria and procedures outlined in the Guide may be granted an "SSV" notation to indicate compliance.[285]

Volume 5 is designed to augment ABS's *Guide for Integrated Software Quality Management (ISQM)*.[286] The *ISQM* "presents a risk-based software development and maintenance process . . . based upon internationally recognized standards."[287] This volume is designed mainly for software system providers involved in software design and quality assurance.[288]

[279] American Bureau of Shipping, *Guide for: Software Systems Verification*, 4 ABS CYBERSAFETY™ ii (2016), http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/253_cybersafetyV4/CyberSafety_V4_SSV_Guide_e.pdf.
[280] *Id.* at 1.
[281] *Id.* at 6.
[282] *Id.* at 3. *Id.* at 3. A Verification and Validation Organization (V&V) is "[t]he organization that develops the verification plan and performs the software verification of the control system." The V&V must be an independent third party unless "special consideration" is requested from ABS and ABS determines that "sufficient independence" exists between the V&V and the system provider of the software being verified.
[283] *Id.* at 13–14; Occupational Safety & Health Admin., *Oil and Gas Well Drilling and Servicing eTool: Drilling—Blowout Preventers*, U.S. DEP'T OF LABOR, https://www.osha.gov/SLTC/etools/oilandgas/drilling/wellcontrol_bop.html (last visited Feb. 11, 2017) (a blowout preventer is designed to prevent blowout from occurring on an oil or gas well by "shut[ting] off the well hole and prevent[ing] the escape of the underground fluids").
[284] 4 AMERICAN BUREAU OF SHIPPING, *supra* note 278 at 8.
[285] *Id.* at 1.
[286] 5 AMERICAN BUREAU OF SHIPPING, ABS CYBERSAFETY™ GUIDANCE NOTES ON SOFTWARE PROVIDER CONFORMITY PROGRAM ii (2016), http://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/254_cybersafetyV5/CyberSafety_V5_SPCP_GN_e.pdf.
[287] *Id.*
[288] *Id.* at 1.

The ABS standards are by far the most detailed and thorough currently available in the maritime domain. ABS, as a classification society, carries great weight in the maritime industry. "In the absence of classification societies for ships, there would be no benchmark or guideline standards for vessels and other constructions to adhere to." [289] Thus, the ABS CyberSafety™ Guidance Notes are a big step forward for the cybersecurity practices of the maritime industry and should be used as a template for future industry tactics, techniques, and procedures. Wide adoption of the ABS standards and creation of similar standards by other classification societies will allow the maritime industry to vastly improve cybersecurity awareness and preparation, effectively reducing cyber vulnerabilities.

IV. RECOMMENDATIONS

Recently the U.S. government and the maritime industry have made good strides towards addressing cybersecurity issues in the maritime domain. However, while a good foundation currently exists, the industry and government need to continue to build on that foundation. The next steps include creating a pervasive culture of cyber risk awareness, ensuring that to the extent possible, MTSA required security plans address cyber risk, and revising current regulations or developing new regulations to focus on cybersecurity.

A. *Create a Culture of Cyber Risk Awareness*

All components of the marine transportation sector—government, port facilities, ship owners and operators, and other related entities—need to create a culture of cyber risk awareness. This culture needs to be supported by the highest levels of management and continue down through all personnel who access systems vulnerable to cyber-attack. Indeed, the BIMCO Guidelines specifically state that "[c]yber security should start at the senior management level of a company . . . ."[290] The key to implementing such a culture is educating personnel on cyber vulnerabilities and types of threats. All of the materials reviewed for this Note advocated the creation of a total organizational culture that promoted cyber risk awareness. Until this type of culture is in place, and robust cyber awareness training and education is the norm, each organization is only as safe as its least educated employee with access to critical systems.

B. *Ensure MTSA Required Plans Address Cyber Risk*

The requirements promulgated under MTSA for area maritime, facility, and vessel security plans can be considered to include cyber elements through the communications and security systems section.[291] In creating, updating, and evaluating vessel and facility security plans, emphasis should be placed on ensuring that cyber vulnerabilities are considered and addressed. The Coast Guard and AMS Committees should make addressing cyber risk a top priority.

---

[289] Sharda, *The Importance of Classification Societies in the Maritime Industry*, MARINE INSIGHT (July 21, 2016), http://www.marineinsight.com/maritime-law/the-importance-of-classification-societies-in-the-maritime-industry/.
[290] BALTIC & INT'L MAR. COUNCIL, *supra* note 249 at 6.
[291] 33 C.F.R. §§ 103.405, 104.405, 105.405 (2016).

The NIST Framework is a useful tool for companies and organizations to use in evaluating current approaches to cybersecurity. The Coast Guard, AMS Committees, classification societies, and maritime organizations should encourage use of the Framework when addressing cyber risk. The procedures put in place based on NIST Tiers and Profiles should be included in all MTSA required plans.

Once MTSA required plans include cyber elements, the planned response to cyber-attacks should be regularly tested through drills and exercises. This will help ensure that employees and regulators are familiar with the policies and procedures set forth in the plans. It will also help identify any gaps in the plans. Identifying gaps in an environment where the risk is simulated and failure does not cause irreparable damage is preferable to discovering gaps during an actual attack. Furthermore, it will allow individuals who have been identified in the plans as having decision-making authority to practice making decisions related to cyber-attacks.

The Port Security Grant Program (PSGP) should continue to emphasize cybersecurity as a critical priority. This funding opportunity can assist maritime companies and port stakeholders in paying for third-party assessments, or gaining equipment needed to close cyber vulnerabilities identified in such assessments.[292] However, FEMA should ensure appropriate standards are promulgated for review of cyber projects under the PSGP. These standards should include provisions to allow both field and national level reviewers to consult with appropriate cyber experts during the review process.

C. *Develop Additional Maritime Focused Cybersecurity Legislation*

While MTSA can be read to include cyber, it would be better to either pass legislation that amended MTSA to explicitly include cybersecurity, or create new legislation specifically focused on cybersecurity in the maritime sector. Legislation designed to revise and amend MTSA would clearly signal that cyber threats and vulnerabilities are an important part of the security of United States seaports and vessels. Even MTSA was an amendment to an earlier act (the Merchant Marine Act of 1936).[293] Any revision of MTSA should update the definition of a transportation security incident to clearly include cyber-related disruptions.[294] Additionally, any revision of MTSA (or new legislation) should include a requirement for vessels and facilities to create, test, and maintain plans to address cybersecurity vulnerabilities and responses to cyber-attacks.

[292] *See e.g. DHS Needs to Enhance Efforts to Address Port Cybersecurity*, *supra* note 92 at 9.
[293] Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, 116 Stat. 2064 (2002).
[294] *See* U.S. Coast Guard, *supra* note 163.

2014 and 2015 saw a significant increase in cybersecurity legislation.[295] However, many additional governmental cybersecurity polices were promulgated by Executive Order and Presidential Policy Directive. With a major change in administration occurring in January 2016, it is unknown how many of these policies and procedures will remain in effect or what focus the new administration will have on cybersecurity.[296] This uncertainty highlights the need for the creation of additional, durable cybersecurity legislation. The policies enacted through Executive Order and Presidential Policy Directive should be considered for inclusion in new or revised legislation. This way, the best and most effective of the practices identified in these presidential orders can be codified into legislation. This will allow such policies to endure even in the face of presidential transition.

V. CONCLUSION

Modern ships, facilities, and ports rely on integrated systems that are vulnerable to cyber-attacks. Thankfully, a major cyber-attack on the marine transportation sector has not yet occurred. However, significant manmade disruptions have shown the far-reaching effects such events could have on the prosperity and security of the United States.[297] The capabilities of cyber-terrorists are continuing to grow and develop, presenting increased risks to the industrial control systems employed by the maritime industry. Both the maritime industry and the federal government have begun to address the cyber threat in the maritime domain. However, both the industry and government need to continue building on this foundation and harden marine transportation against cyber threats. It is critical for all maritime partners to implement a culture of cyber risk awareness. This culture must be pervasive, reaching from the highest levels of management to the workers at the most junior levels. Additionally, the government should work with industry to share information, leverage current regulations to their full extent, and create new regulations that specifically focus on cybersecurity. Only through continuous vigilance and a willingness to share information will the marine transportation sector be able to protect its critical intellectual property and keep ports, facilities, and vessels safe from cyber threats.

[295] *See supra* Part II.C. Prior to 2014 no significant cybersecurity legislation had been enacted since 2002, however, in 2014 five Acts were approved and another major Act was passed in 2015.
[296] Joseph J. Lazzarotti, *President Donald J. Trump—What Lies Ahead for Privacy, Cybersecurity, e-Communication?*, 11/9/16 NAT'L L. REV., 2016 WLNR 34340881 (2016).
[297] *See supra* Part I.A.

Cybaris®

Cybaris®, an Intellectual Property Law Review, publishes non-student articles and student comments on all areas of intellectual property law, including patents, copyrights, trademarks, licensing, and related transactional matters.
mitchellhamline.edu/cybaris

Intellectual Property Institute

Cybaris® is a publication of the Intellectual Property Institute at Mitchell Hamline School of Law.
mitchellhamline.edu/ip

MITCHELL | HAMLINE
School of Law

875 Summit Avenue, Saint Paul, MN 55105
mitchellhamline.edu